II. AMENDMENTS TO THE CLAIMS:

This listing of claims replaces all prior versions, and listings, of claims of the application.

1. (Currently Amended) A data management system, comprising:

an access control system for limiting access to the data management system to authorized entities;

a data confidentiality system for identifying details in ~~the~~ received data as one of secret, temporarily secret, possibly secret, and not secret, wherein secret, temporarily secret and possibly secret comprise confidential details and concealing confidential details in received data from a requester while allowing a composite analysis to be performed by the requester that is based on the confidential details;

a data storage system for storing the received data; and

a data update system for periodically automatically examining stored data to identify and expose any confidential details that have become non-confidential details.

2. (Original) The system of claim 1, further comprising:

a data decryption system for decrypting received data;

a data verification system for verifying an accuracy of received data;

a program approval system for approving systems for analyzing the stored data; and

a key security system for protecting encryption keys.

3. (Original) The system of claim 1, wherein stored data is analyzed with a data analysis system.

4. (Original) The system of claim 3, wherein the data analysis system is permitted to analyze the stored data based upon approval by full rights members of the data management system.

5. (Original) The system of claim 1, wherein data management system is a tamper resistant, tamper evident, tamper sensitive, tamper reactive, and programmable system.

6. (Original) The system of claim 1, wherein the received data and the stored data are operational risk data.

7. (Original) The system of claim 1, wherein the system mitigates operational risk.

8. (Original) The system of claim 1, wherein data is received based upon a randomly generated time interval.

9. (Original) The system of claim 1, wherein the confidential details cannot be accessed by any entity.

10. (Original) The system of claim 1, wherein the confidential details can only be accessed by a plurality of entities acting in concert.

11. (Original) The system of claim 1, further comprising a customer relationship management tool for verifying a policy of an entity.

12. (Currently Amended) A data management system, comprising:

an access control system for limiting access to the data management system to authorized entities;

a data decryption system for receiving at randomly generated time intervals and decrypting received operational risk data;

a data confidentiality system for identifying details in the received data as one of secret, temporarily secret, possibly secret and not secret, wherein secret, temporarily secret and possibly secret comprise confidential details and concealing confidential details in the received data from a requester while allowing a composite analysis to be performed by the requester that is based on the confidential details;

a data storage system for storing received data after the confidential details have been concealed;

a data update system for periodically examining stored data to identify and expose any confidential details that have become non-confidential details;

a program approval system for approving systems for analyzing the stored data; and

a key security system for protecting encryption keys.

13. (Original) The system of claim 12, wherein stored data is analyzed with a data analysis system.

14. (Original) The system of claim 13, wherein the data analysis system is permitted to analyze the stored data by the program approval system based upon approval by full rights members of the data management system.

15. (Original) The system of claim 12, wherein a provider submits the operational risk data to the data management system, and wherein a requester accesses the stored data.

16. (Currently Amended) A method for managing data, comprising:

receiving operational risk data at randomly generated time intervals in a secured manner from an authorized provider;

identifying details in the received data as one of secret, temporarily secret, possibly secrete and not secret, wherein secret, temporarily secret and possibly secret comprise confidential details and concealing confidential details in the received data from a requester while allowing a composite analysis to be performed by the requester that is based on the confidential details;

storing the received data; and

updating the stored data by identifying and exposing any confidential details that have become non-confidential details in the stored data.

17. (Previously Presented) The method of claim 16, further comprising:

decrypting the received data, prior to the identifying step;

verifying an accuracy of the received data;

approving a system for analyzing the stored data; and

protecting encryption keys.

18. (Original) The method of claim 16, further comprising analyzing the stored data with a data analysis system.

19. (Original) The method of claim 18, further comprising approving the data analysis system based upon approval by full rights members.

20. (Currently Amended) A program product, stored on a computer readable medium, for managing data, which when executed, comprises:

an access control system for limiting access to the data management system to authorized entities;

a data confidentiality system for identifying details in ~~the~~ received data as one of secret, temporarily secret, possibly secret and not secret, wherein secret, temporarily secret, and possibly secret comprise confidential details and concealing confidential details in the received data from a requester while allowing a composite analysis to be performed by the requester that is based on the confidential details;

a data storage system for storing the received data; and

a data update system for periodically examining stored data to identify and expose any confidential details that have become non-confidential details.

21. (Original) The program product of claim 20, further comprising:

a data decryption system for decrypting received data;

a data verification system for verifying an accuracy of received data;

a program approval system for approving systems for analyzing the stored data; and

a key security system for protecting encryption keys.

22. (Original) The program product of claim 20, further comprising a data analysis system for analyzing the stored data.

23. (Original) The program product of claim 20, wherein the data analysis system is approved by full rights member.

24. (Original) The program product of claim 20, wherein the received data is operational risk data.